CLAIMS

What is claimed is:

1. A method of implementing a password checking function based on password-related data in a directory server system comprising:

organizing a plurality of user entries in a tree structure;

creating an additional entry, having attached password-related data;

attaching extra data to a given user entry, the extra data designating the additional entry; and

upon a call of the password checking function for the given entry, executing the password policy checking function for the given user entry based on the password-related data in the additional entry designated by the extra data of the given user entry.

2. The method of claim 1, wherein:

the additional entry has a scope in the tree structure; and

executing the password policy checking function is performed subject to the given user entry belonging to the scope of the additional entry.

3. The method of claim 2, wherein the scope of the additional entry comprises the subtree of the parent entry of that additional entry.

4. The method of claims 1, wherein the additional entry has at least one attribute, whose value contains password-related data.

5. The method of claim 4, wherein the value of said at least one attribute contains password policy data.

6. The method of claims 1, wherein creating an additional entry comprises attaching an object class data to an additional entry, said object class data identifying a predefined object class associated with said password-related data.

7. The method of claims 1, wherein attaching extra data to a given user entry further comprises checking whether the tree structure comprises the additional entry, as identified by the extra data.

8. The method of claim 2, wherein:

creating an additional entry comprises creating a plurality of additional entries, each having attached password-related data, the additional entries having different scopes in the tree structure, and

executing the password policy checking function is performed subject to the given user entry belonging to the scope of one of the additional entries.

9. The method as claimed in claim 8, further comprising:

executing the password policy checking function on the given user entry, using predefined password related data, when the given user entry has no extra data associated thereto.

10. The method of claim 1, wherein the extra data designates the location of said additional entry.

11. The method of claim 1, wherein attaching extra data to a given user entry comprises directly adding the extra data to the given user entry.

12. The method of claim 11, wherein attaching extra data to a given user entry further comprises adding the extra data to the given user entry in the form of an extra data attribute whose value designates the location of the additional entry.

13. The method of claim 12, wherein the extra data attribute is an operational attribute.

14. The method of claim 1, wherein:

the directory server has a class of service mechanism; and

attaching extra data to a given user entry comprises adding the extra data in the form of a class of service being applicable to one or more user entries.

15. The method of claim 14, wherein a class of service has a scope and said one or more user entries are located in the scope of the class of service.

16. The method of claim 15, wherein the scope of a class of service comprises the entries located in the subtree of the parent entry of an entry defining the class of service.

17. The method of claims 14, wherein:

the directory server has a role mechanism; and

attaching extra data to a given user entry comprises adding the extra data to a class of service being applicable to one or more user entries having the same role.

18. The method of claims 14, wherein creating an additional entry comprises adding said additional entry in the same level of the tree as the entry defining the class of service.

19. A computer-readable medium containing a plurality of instructions which when executed cause a directory server to provide a method of configuring password policies in a directory server system comprising:

organizing a plurality of user entries in a directory information tree;

creating an additional user entry in said directory information tree; and

attaching a given password policy to said additional user entry, wherein the password policy comprises;

an attribute attached to said additional user entry identifying said given password policy; and

an attribute value comprising a password policy rule.

20. The computer-readable medium according to Claim 19, wherein said attribute of said given password policy is operative and is not associated with an object class in a schema.

21. The computer-readable medium according to Claim 19, wherein said attribute of said given password policy comprises a corresponding distinguished name syntax attached to said additional user entry.

22. The computer-readable medium according to Claim 19, wherein said attribute of said given password policy is generated by a class of server.

23. The computer-readable medium according to Claim 22, wherein said attribute value of said password policy is based on a role possessed by said user entry.

24. The computer-readable medium according to Claim 19, wherein said password policy attribute is real.

25. The computer-readable medium according to Claim 24, wherein said attribute and said attribute value are defined in said user entry.

26. A computer-readable medium containing a plurality of instructions which when executed cause a directory server to implement a password policy checking method comprising:

receiving a binding request;

retrieving a corresponding user entry;

determining if said corresponding user entry has a password policy subentry attribute;

retrieving a password policy entry corresponding to said password policy subentry attribute, if said user entry has said password policy subentry attribute;

determining if said password policy entry is present;

retrieving a password policy subentry attribute value, if said user entry has said password policy subentry attribute and if said password policy entry is present; and

executing said password policy checking as a function of said password policy attribute value corresponding to said user entry, if said user entry has said password policy subentry attribute and if said password policy entry is present.

27. The computer-readable medium according to Claim 26, further comprising:

retrieving a default password policy entry if said user entry does not have a password policy subentry attribute or if said password policy is not present;

determining if said default password policy entry is present, if said user entry does not have a password policy subentry attribute or if said password policy is not present;

retrieving a hard-coded password policy attribute value, if said user entry does not have a password policy subentry attribute or if said password policy is not present, and if said default password policy is not present; and

executing said password policy checking as a function of said hard-coded password policy attribute value, if said user entry does not have a password policy subentry attribute or if said password policy is not present, and if said default password policy is not present.

28. The computer-readable medium according to Claim 26, further comprising:

retrieving a default password policy entry if said user entry does not have a password policy subentry attribute or if said password policy is not present;

determining if said default password policy entry is present, if said user entry does not have a password policy subentry attribute or if said password policy is not present;

retrieving a default password policy attribute value, if said user entry does not have a password policy subentry attribute or if said password policy is not present, and if said default password policy is present; and

executing said password policy checking as a function of said default password policy attribute value, if said user entry does not have a password policy subentry attribute or if said password policy is not present, and if said default password policy is present.

29. The computer-readable medium according to Claim 28, further comprising:

retrieving a default password policy entry if said user entry does not have a password policy subentry attribute or if said password policy is not present;

determining if said default password policy entry is present, if said user entry does not have a password policy subentry attribute or if said password policy is not present;

retrieving a hard-coded password policy attribute value, if said user entry does not have a password policy subentry attribute or if said password policy is not present, and if said default password policy is not present; and

executing said password policy checking as a function of said hard-coded password policy attribute value, if said user entry does not have a password policy subentry attribute or if said password policy is not present, and if said default password policy is not present.